IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Owlett et al.	Group Art Unit: 2433 / Conf. # 6660
Application No.: 10/539,648	Examiner: Woldemariam, Nega
Filing Date: 12/17/2007	Docket No.: GB920020055US1

Title: **METHODS, APPARATUS AND COMPUTER PROGRAMS FOR GENERATING AND/OR USING CONDITIONAL ELECTRONIC SIGNATURES FOR REPORTING STATUS CHANGES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

This Appeal Brief, pursuant to the Notice of Appeal filed August 10, 2010, is an appeal from the rejection of the Examiner in the Final Office Action mailed February 17, 2010.

REAL PARTY IN INTEREST

International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1 and 27-31, 34-39, and 42-47 are finally rejected. Claims 2-26, 32-33, 40-41 and 48-49 are canceled. The rejection of claims 1, 27-31, 34-39, and 42-47 is being appealed.

STATUS OF AMENDMENTS

The amendment filed April 19, 2010 in response to the Final Office Action mailed February 17, 2010 is entered as indicated in the Advisory Action mailed July 12, 2010.

SUMMARY OF CLAIMED SUBJECT MATTER

CLAIM 1 - INDEPENDENT

The present invention provides a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item (specification, page 3, lines 7-10).

The data item (10, Figure 3) is hashed (40, Figure 3) to generate a digest (50, Figure 3) of the data item. See lines 1-2 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

Each condition (20, 200, Figure 3) of the one or more conditions is separately hashed from each other and separately from the data item to generate one or more condition digests (50, 210, Figure 3) respectively corresponding to the one or more conditions. See lines 2-4 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

A reference digest is set equal to the digest of the data item. See line 11 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

A computer iteratively processes a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digest, each unique condition digest being a different condition digest in each iteration of the loop. See lines 8-20 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

Said processing in each iteration comprises concatenating (60, Figure 3) the reference digest with the unique condition digest of the iteration to generate a concatenand (70, Figure 3) and hashing (80, Figure 3) the concatenand to generate a hashed concatenand (90, Figure 3) that serves as the reference digest for the next iteration if the next iteration is performed. See lines 11-15 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

The regenerated reference digest of the last iteration of the loop being a last digest (200, Figure 3). See lines 19-20 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

The last digest is encrypted (100, Figure 3) to generate a digital signature block (260, Figure 3) that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature, wherein the one or more conditions is a plurality of conditions (20, 200, FIG. 3). See lines 22-27 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

<u>CLAIM 34 - INDEPENDENT</u>

The present invention provides a computer program product, comprising a machine-readable recording medium (specification, page 11, lines 37-39), having program code (350, 360, Figure 4) recorded thereon said program code upon being executed by a data processing apparatus (specification, page 10, lines 36-39) causes the data processing apparatus to perform a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item (specification, page 3, lines 7-10).

The data item (10, Figure 3) is hashed (40, Figure 3) to generate a digest (50, Figure 3) of the data item. See lines 1-2 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

Each condition (20, 200, Figure 3) of the one or more conditions is separately hashed from each other and separately from the data item to generate one or more condition digests (50, 210, Figure 3) respectively corresponding to the one or more conditions. See lines 2-4 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

A reference digest is set equal to the digest of the data item. See line 11 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

The data processing apparatus iteratively processes a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digest, each unique condition digest being a different condition digest in each iteration of the loop. See lines 8-20 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

Said processing in each iteration comprises concatenating (60, Figure 3) the reference digest with the unique condition digest of the iteration to generate a concatenand (70, Figure 3) and hashing (80, Figure 3) the concatenand to generate a hashed concatenand (90, Figure 3) that serves as the reference digest for the next iteration if the next iteration is performed. See lines 11-15 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

The regenerated reference digest of the last iteration of the loop being a last digest (200, Figure 3). See lines 19-20 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

The last digest is encrypted (100, Figure 3) to generate a digital signature block (260, Figure 3) that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature, wherein the one or more conditions is a plurality of conditions (20, 200, FIG. 3). See lines 22-27 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

<u>CLAIM 42 - INDEPENDENT</u>

The present invention provides a data processing apparatus (specification, page 10, lines 36-39) comprising a computer (300, FIG. 4) and a machine-readable recording medium (specification, page 11, lines 37-39), coupled to the computer, said recording medium storing program code (350, 360, Figure 4) that when executed by the computer causes the computer to perform a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item (specification, page

3, lines 7-10).

The data item (10, Figure 3) is hashed (40, Figure 3) to generate a digest (50, Figure 3) of the data item. See lines 1-2 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

Each condition (20, 200, Figure 3) of the one or more conditions is separately hashed from each other and separately from the data item to generate one or more condition digests (50, 210, Figure 3) respectively corresponding to the one or more conditions. See lines 2-4 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

A reference digest is set equal to the digest of the data item. See line 11 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

The data processing apparatus iteratively processes a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digest, each unique condition digest being a different condition digest in each iteration of the loop. See lines 8-20 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

Said processing in each iteration comprises concatenating (60, Figure 3) the reference digest with the unique condition digest of the iteration to generate a concatenand (70, Figure 3) and hashing (80, Figure 3) the concatenand to generate a hashed concatenand (90, Figure 3) that serves as the reference digest for the next iteration if the next iteration is performed. See lines 11-15 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

The regenerated reference digest of the last iteration of the loop being a last digest (200, Figure 3). See lines 19-20 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

The last digest is encrypted (100, Figure 3) to generate a digital signature block (260, Figure 3) that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature, wherein the one or more conditions is a plurality of conditions (20, 200, FIG. 3). See lines 22-27 in paragraphs added between lines 35 and 36 of page 9 of specification, as specified in preliminary amendment filed 06/16/2005.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1 and 27-49 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Ishibashi et al. US Publication No.: 7,099,846 B1 (hereinafter Ishibashi) in view of Sudia et al. US Patent No. 5,995,625 (hereinafter Sudia).

ARGUMENT

<u>GROUND OF REJECTION 1</u>

Claims 1 and 27-49 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Ishibashi et al. US Publication No.: 7,099,846 B1 (hereinafter Ishibashi) in view of Sudia et al. US Patent No. 5,995,625 (hereinafter Sudia).

<u>Claims 1, 34, and 42</u>

Appellants respectfully contend that claims 1, 34, and 42 are not unpatentable over Ishibashi in view of Sudia, because Ishibashi in view of Sudia does not teach or suggest each and every feature of claims 1, 34, and 42.

A first example of why claims 1, 34, and 42 are not unpatentable over Ishibashi in view of Sudia is that Ishibashi in view of Sudia does not teach or suggest the feature: "hashing the data item to generate a digest of the data item; ... setting a reference digest equal to the digest of the data item; ... said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand".

The Examiner argues: "As to claim 1, Ishibashi teaches ... **the data item to generate a digest of the data item** (see Ishibashi col. 15 lines 5—7, generating message/data digest); ... **setting a reference digest equal to the digest of the data item** (see Ishibashi col.23 lines 20—25 and Fig. 26, electronic signatures stored for conditions to the information/data item); ... Sudia teaches ... **said processing in each iteration comprising concatenating the reference**

digest with the unique condition digest of the iteration to generate a concatenand ... (see Sudia Fig. 2, Fig. 8 and col. 8 line 55—59, a hash of the acceptance phrase/condition is combined/concatenated with a hash of the issuing policy statement/condition repeatedly with other key information such as random value to form key value)".

In response, Appellant asserts that the phrases "the digest of the data item"and "a digest of the data item" refer to the same data item due to antecedent basis considerations of "the digest of the data item" with respect to "a digest of the data item". Therefore, due to the rules of antecedent basis, the "data item" in the "setting" step must be the same "data item" as in the first iteration of the loop, which is violated by the combination of Ishibashi and Sudia.

Specifically, the "data item" referred in the Examiner's citations to Ishibashi col. 15 lines 5-7 and col. 23, lines 20-25 is an electronic signature. In contrast, the "data item" referred in the Examiner's citation to Sudia, col. 8, line 55-59 is an acceptance phrase/condition, an issuing policy statement/condition, or a random value. Therefore, the combination of Ishibashi and Sudia does not disclose the same "data item" in the "setting" step as in the first iteration of the loop, in violation of antecedent basis constraints imposed on claims 1, 34, and 42.

Therefore, Ishibashi in view of Sudia does not disclose the preceding feature of claims 1, 34, and 42.

A second example of why claims 1, 34, and 42 are not unpatentable over Ishibashi in view of Sudia is that Ishibashi in view of Sudia does not teach or suggest the feature: "said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand".

The Examiner argues: "Sudia teaches ... **said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand** ... (see Sudia Fig. 2, Fig. 8 and col. 8 line 55—59, a hash of the acceptance phrase/condition is combined/concatenated with a hash of the issuing policy statement/condition repeatedly with other key information such as random value to form key value)".

In response, Appellants note that Sudia, col. 8, lines 55-59 recites: "A hash of the acceptance phrase 66' is then ***combined*** with a hash of the issuing CA policy statement 64 (and, if appropriate, the other key information, for example, a random value, 58 obtained from the certificate 38) to form a key value KV' 62'." (emphasis added)

Appellants assert that the preceding quote from Sudia, col. 8, lines 55-59 does not discloses ***concatenating*** hashes as claimed, bur rather discloses ***combining*** hashes. Appellants assert that the scope of "combining" is broader than "concatenating". For example, two hashes may be combined by any logical operator such as AND, OR, NOR, NAND, etc. Thus, Sudia, col. 8, lines 55-59 does not discloses concatenating hashes as claimed

Therefore, Ishibashi in view of Sudia does not disclose the preceding feature of claims 1, 34, and 42.

A third example of why claims 1, 34, and 42 are not unpatentable over Ishibashi in view of Sudia is that Ishibashi in view of Sudia does not teach or suggest the feature: "iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests, ***said processing***

in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed, each unique condition digest being a different condition digest in each iteration of the loop, the regenerated reference digest of the last iteration of the loop being a last digest ..., wherein the one or more conditions is a plurality of conditions".

Thus, the preceding claimed feature requires:

(i) the initially set reference digest is the hash of the data item;

(ii) the hashed concatenand computed in iteration 1 is a concatenation of the initially set reference digest and a first unique condition digest;

(iii) the hashed concatenand computed in iteration 2 is a concatenation of the hashed concatenand computed in iteration 1 and a second unique condition digest;

(iv) the hashed concatenand computed in iteration 3 is a concatenation of the hashed concatenand computed in iteration 2 and a third unique condition digest; etc.

Thus, the preceding claimed feature requires that the hashed concatenand computed in iteration N is a concatenation of the hashed concatenand computed in iteration N-1 and a Nth unique condition digest, which Sudia does not disclose.

The Examiner relies on Sudia as allegedly disclosing the preceding feature of claims 1, 34, and 42. In particular, the Examiner argues: "Sudia teaches(see Fig. 1, and col. 7 lines 30—35 unique conditions, acceptance phrase and optionally other data can first be combined and then their combination can be digested repeatedly/iteratively)".

In response, Appellants assert that Sudia, FIG. 1 discloses that a wrap key 30 is computed (e.g., in a first iteration) as a combination of digest of conditions 14, a digest of acceptance phrase 20, and a digest of other data 26, and the wrap key 30 is used to wrap data 32 to generate wrapped data 36 (see also Sudia, col. 6, lines 18-22). Sudia does not disclose that the wrap key computed in the second iteration is computed as a combination of the wrap key computed in the first iteration and other parameters (a digest of conditions 14, a digest of acceptance phrase 20, a digest of other data 26).

The Examiner also cites Sudia, col. 19, lines 57-67. To comprehend the preceding citation by the Examiner, Appellants note that Sudia, col. 19, lines recite : "If the wrapped digital data consists of a signature on a specific business transaction, the wrapping process can require the recipient to obtain additional information from a third party. For example, the sender who wraps the digital data may possess a document from a third party pertaining (for example) to the subsequent use of the wrapped digital data. This agreement may be hashed in computing the wrap and unwrap keys, so that the recipient of the wrapped signature must also obtain that additional documentation from the third party and agree to its contents when computing the unwrap key. ***That document could in turn also be wrapped (either in its entirety, or as to its signature) under another set of conditions***, giving rise to a chain of conditions that must be assented to in order to validate the wrapped signature on the first transaction. If the additional document were to contain a sequentially numbered value along with a random value, then the recipient's use of a series of wrapped data messages can be made contingent on obtaining a series of numbered documents from a third party. This has significant implications for the design of cryptographic transaction control systems." (emphasis added)

Appellants respectfully contend that the preceding quote from Sudia, col. 19, lines 57-67 does not disclose that the wrap key computed in the second iteration is computed as a combination of the wrap key computed in the first iteration and other parameters (a digest of conditions 14, a digest of acceptance phrase 20, a digest of other data 26). Rather, the wrap key computed in the second iteration is computed as a combination of the document (or the document's signature) another set of conditions 10 (and possibly parameters such as a digest of acceptance phrase 16 and a digest of other data 22). Sudia, col. 19, lines 57-67 does not disclose that the wrap key computed in one iteration is combined with other data to compute another wrap key in a next iteration.

In the Advisory Action, the Examiner also cites Sudia, col. 17, lines 10-14. To comprehend the preceding citation by the Examiner, Appellants note that Sudia, col. 17, lines 8-21 recite: "When recording the glyph value, UID, and buyer identification in the database, the seller may protect the integrity of those database entries by a method of hash chaining, such as by including a hash of the previous database record in the current one, and then including a hash of the current record in the next record, and so on, as is known in the prior art... Thus, with reference to FIGS. 1 and 3, data 32 can be watermarked digital data or digital data with a glyph, and the watermark or glyph is used as part of the other data 22 when forming the wrap key value 30 (or unwrap key value 30')."

Appellants respectfully contend that the preceding quote from Sudia, col. 17, lines 8-21 does not disclose that the wrap key computed in the second iteration is computed as a combination of the wrap key computed in the first iteration and other parameters. Rather, the other data 22 is a database record that is hashed in each iteration and then the hash of the database record of other data 22 is combined in the next iteration with the digest of conditions

14, the digest of acceptance phrase 20, and the digest of other data 26. Sudia, col. 17, lines 8-21 does not disclose that the wrap key computed in one iteration is combined with other data to compute another wrap key in a next iteration.

Therefore, Ishibashi in view of Sudia does not disclose the preceding feature of claims 1, 34, and 42.

A fourth example of why claims 1, 34, and 42 are not unpatentable over Ishibashi in view of Sudia is that Ishibashi in view of Sudia does not teach or suggest the feature: "the regenerated reference digest of the last iteration of the loop being a last digest; and encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature, wherein the one or more conditions is a plurality of conditions".

The Examiner argues: "Sudia teaches ... **the regenerated reference digest of the last iteration of the loop being last digest** (see Sudia col. 19 lines 57—67, wrapped signature/digest condition, product or data be wrapped creating a series of wrapped data); **and encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature** (se Sudia Fig. 8 and col. 11 lines 45-64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)".

In response, Appellants assert that the language of claims 1, 34, and 42 requires the last reference digest to be the value of the wrap key 30 in Sudia, FIG. 1 computed in the last iteration, because the reference digest in each iteration is claimed to be a hashing of the concatenation of the reference digest of the preceding iteration and the unique condition digest. However, the preceding claimed feature requires the last reference digest to be signed with a digital signature, and Sudia does not disclose that the wrap key 30 is signed with a digital signature. To the contrary, Sudia, col. 6, lines 22-23 discloses that the wrap key 30 is used to wrap the data 32 to produce the wrapped data 36.

Therefore, Ishibashi in view of Sudia does not disclose the preceding feature of claims 1, 34, and 42.

Based on the preceding arguments, Appellants respectfully maintain that claims 1, 34, and 42 are not unpatentable over Ishibashi in view of Sudia, and that claims 1, 34, and 42 are in condition for allowance.

Claims 27, 35, and 43

Since claims 27, 35, and 43 respectively depend from claims 1, 34, and 42 which Appellants have argued *supra* to not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a), Appellants maintain that claims 27, 35, and 43 are not unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

In addition with respect to claims 27, 35, and 43, Appellants assert that Ishibashi in view of Sudia does not disclose the feature: "wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions".

The Examiner argues: “As to 27, the combination of Ishibashi and Sudia teaches **the method, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions** (see Sudia col. 2 lines 61-65, a particular pass phrase indicating acceptance of conditions of digital data)”.

In response, Appellants assert that the Examiner’s allegation that a particular pass phrase indicates acceptance of conditions of digital data is unrelated to the claimed limitation that the signer performs signing the last digest with a digital certificate (see claims 1, 34, and 42). Thus, the Examiner’s argument does not make sense and is therefore not persuasive.

Accordingly, claims 27, 35, and 43 are not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

Claims 28, 36, and 44

Since claims 28, 36, and 44 respectively depend from claims 1, 34, and 42 which Appellants have argued *supra* to not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a), Appellants maintain that claims 28, 36, and 44 are not unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

In addition with respect to claims 28, 36, and 44, Appellants assert that Ishibashi in view of Sudia does not disclose the feature: “wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions”.

The Examiner argues: “As to 28, the combination of Ishibashi and Sudia teaches **the method, wherein said signing is performed by a signer and represents acceptance of the**

data item by the signer, and wherein said acceptance is not subject to the one or more conditions (see Sudia col. 8 lines 32—42 the subscriber accept and digitally sign acceptance of conditions)".

In response, Appellants assert that the Examiner's allegation that the subscriber accepts and digitally signs acceptance of conditions is unrelated to the claimed limitation that the signer performs signing the last digest with a digital certificate (see claims 1, 34, and 42). Thus, the Examiner's argument does not make sense and is therefore not persuasive.

Accordingly, claims 28, 36, and 44 are not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

<u>Claims 29, 37, and 45</u>

Since claims 29, 37, and 45 respectively depend from claims 1, 34, and 42 which Appellants have argued *supra* to not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a), Appellants maintain that claims 29, 37, and 45 are not unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

In addition with respect to claims 29, 37, and 45, Appellants assert that Ishibashi in view of Sudia does not disclose the feature: "generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and sending the communication across a network to a recipient".

The Examiner argues: "As to 29, the combination of Ishibashi and Sudia teaches **the method, said method further comprising: generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more**

conditions; and sending the communication across a network to a recipient (see Sudia col. 19, lines 37—46, sending wrapped digital data and conditions over a network including digital signature)".

In response, Appellants respectfully contend that the preceding claimed feature requires sending a communication across a network to a recipient. The communication must comprise the digital signature block, the data item, and the one or more conditions, which is not disclosed in Sudia col. 19, lines 37-46. Appellants assert that Sudia col. 19, lines 37-46 discloses sending the wrapped digital data 22 and conditions to the recipient, but does not disclose sending the digital signature block to the recipient.

Accordingly, claims 29, 37, and 45 are not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

Claims 30, 38, and 46

Since claims 30, 38, and 46 respectively depend from claims 1, 34, and 42 which Appellants have argued *supra* to not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a), Appellants maintain that claims 30, 38, and 46 are not unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

In addition with respect to claims 30, 38, and 46, Appellants assert that Ishibashi in view of Sudia does not disclose the feature: generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and sending the communication across a network to a recipient"".

The Examiner argues: "As to 30, the combination of Ishibashi and Sudia teaches **the**

method, said method further comprising: generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and sending the communication across a network to a recipient (see Sudia col. 12, lines 1-7, key value digital signature is sent to verify the wrapped content and condition)".

In response, Appellants respectfully contend that Sudia col. 12, lines 1-7 discloses generating a key value. However, Sudia col. 12, lines 1-7 does not disclose that the generated key value comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions. Furthermore, Sudia col. 12, lines 1-7 does not disclose that the generated key value is sent across a network to a recipient.

Accordingly, claims 30, 38, and 46 are not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

Claims 31, 39, and 47

Since claims 31, 39, and 47 respectively depend from claims 1, 34, and 42 which Appellants have argued *supra* to not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a), Appellants maintain that claims 31, 39, and 47 are not unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

In addition with respect to claims 31, 39, and 47, Appellants assert that Ishibashi in view of Sudia does not disclose the feature:

"hashing a new condition to generate a digest of the new condition;

concatenating the digital signature block with the digest of the new condition to generate a new digest;

hashing the new digest to generate a hashed new digest; and

encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition".

The Examiner argues: "As to 31, the combination of Ishibashi and Sudia teaches **the method, wherein the method further comprises: hashing a new condition to generate a digest of the new condition; concatenating the digital signature block with the digest of the new condition to generate a new digest; hashing the new digest to generate a hashed new digest; and encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition** (se Sudia Fig. 8 and col. 11 lines 45-64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)".

In response, Appellants assert that in in Sudia, FIG. 8, the new conditions 64 are hashed to generate a digest of the new conditions. However, the digital signature block 82 is not concatenated with the hash of the new conditions 64 (i.e., the new digest) as claimed.

Accordingly, claims 31, 39, and 47 are not be unpatentable over Ishibashi in view of Sudia under 35 U.S.C. §103(a).

SUMMARY

In summary, Appellants respectfully requests reversal of the February 17, 2010 Office Action rejection of claims 1 and 27-49.

Date: October 12, 2010

/ Jack P. Friedman /
Jack P. Friedman
Registration No. 44,688

Customer No. 30449
Schmeiser, Olsen & Watts
22 Century Hill Drive - Suite 302
Latham, New York 12110
Telephone (518) 220-1850
Facsimile (518) 220-1857
E-mail: jfriedman@iplawusa.com

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Owlett et al.	Group Art Unit: 2433 / Conf. # 6660
Application No.: 10/539,648	Examiner: Woldemariam, Nega
Filing Date: 12/17/2007	Docket No.: GB920020055US1

Title: **METHODS, APPARATUS AND COMPUTER PROGRAMS FOR GENERATING AND/OR USING CONDITIONAL ELECTRONIC SIGNATURES FOR REPORTING STATUS CHANGES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX A - CLAIMS ON APPEAL

1. A method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item, the method comprising:

hashing the data item to generate a digest of the data item;

hashing each condition of the one or more conditions separately from each other and separately from the data item to generate one or more condition digests respectively corresponding to the one or more conditions;

setting a reference digest equal to the digest of the data item;

a computer iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests, said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed, each unique condition digest being a different condition digest in each iteration of the loop, the regenerated reference digest of the last iteration of the loop being a last digest; and

encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature, wherein the one or more conditions is a plurality of conditions.

27. The method of claim 1, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions.

28. The method of claim 1, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions.

29. The method of claim 1, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and

sending the communication across a network to a recipient.

30. The method of claim 1, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and

sending the communication across a network to a recipient.

31. The method of claim 1, wherein the method further comprises:

hashing a new condition to generate a digest of the new condition;

concatenating the digital signature block with the digest of the new condition to generate a new digest;

hashing the new digest to generate a hashed new digest; and

encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition.

34. A computer program product, comprising a machine-readable recording medium having program code recorded thereon, said program code upon being executed by a data processing apparatus causes the data processing apparatus to perform a method for generating a conditional

electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item, said method comprising:

hashing the data item to generate a digest of the data item;

hashing each condition of the one or more conditions separately from each other and separately from the data item to generate one or more condition digests respectively corresponding to the one or more conditions;

setting a reference digest equal to the digest of the data item;

a data processing apparatus iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests, said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed, each unique condition digest being a different condition digest in each iteration of the loop, the regenerated reference digest of the last iteration of the loop being a last digest; and

encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature, wherein the one or more conditions is a plurality of conditions.

35. The computer program product of claim 34, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions.

36. The computer program product of claim 34, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions.

37. The computer program product of claim 34, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and

sending the communication across a network to a recipient.

38. The computer program product of claim 34, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and

sending the communication across a network to a recipient.

39. The computer program product of claim 34, wherein the method further comprises:

hashing a new condition to generate a digest of the new condition;

concatenating the digital signature block with the digest of the new condition to generate a new digest;

hashing the new digest to generate a hashed new digest; and

encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition.

42. A data processing apparatus comprising a computer and a machine-readable recording medium coupled to the computer, said recording medium storing program code that when executed by the computer causes the computer to perform a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item, said method comprising:

hashing the data item to generate a digest of the data item;

hashing each condition of the one or more conditions separately from each other and separately from the data item to generate one or more condition digests respectively corresponding to the one or more conditions;

setting a reference digest equal to the digest of the data item;

a data processing apparatus iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests, said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed, each unique condition digest being a different condition digest in each iteration of the loop, the regenerated reference digest of the last iteration of the loop being a last digest; and

encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature, wherein the one or more conditions is a plurality of conditions.

43. The data processing apparatus of claim 42, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions.

44. The data processing apparatus of claim 42, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions.

45. The data processing apparatus of claim 42, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and

sending the communication across a network to a recipient.

46. The data processing apparatus of claim 42, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and

sending the communication across a network to a recipient.

47. The data processing apparatus of claim 42, wherein the method further comprises:

hashing a new condition to generate a digest of the new condition;

concatenating the digital signature block with the digest of the new condition to generate a new digest;

hashing the new digest to generate a hashed new digest; and encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Owlett et al.	Group Art Unit: 2433 / Conf. # 6660
Application No.: 10/539,648	Examiner: Woldemariam, Nega
Filing Date: 12/17/2007	Docket No.: GB920020055US1

Title: **METHODS, APPARATUS AND COMPUTER PROGRAMS FOR GENERATING AND/OR USING CONDITIONAL ELECTRONIC SIGNATURES FOR REPORTING STATUS CHANGES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX B - EVIDENCE

There is no evidence entered by the Examiner and relied upon by Appellants in this appeal.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Owlett et al.	Group Art Unit: 2433 / Conf. # 6660
Application No.: 10/539,648	Examiner: Woldemariam, Nega
Filing Date: 12/17/2007	Docket No.: GB920020055US1

Title: **METHODS, APPARATUS AND COMPUTER PROGRAMS FOR GENERATING AND/OR USING CONDITIONAL ELECTRONIC SIGNATURES FOR REPORTING STATUS CHANGES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX C - RELATED PROCEEDINGS

There are no proceedings identified in the "Related Appeals and Interferences" section.